腾讯音乐娱乐 酷狗音乐

个人隐私合规培训

个人隐私监管机构——四部委

- 中央网信办
- 工信部
- 公安部
- 市场监管总局

监管的重要依据，用户投诉要点

- 《网络安全法》第 41 条规定，网络运营者收集、使用个人信息，应当公开收集、使用规则。
- 《消费者权益保护法》第 29 条规定，经营者收集、使用消费者个人信息，“应当公开其收集、使用规则”。

- 具体执行规范：
- GB/T 35273《个人信息安全规范》

历史事件1

- 2019年1月25日，四部委发布《关于开展App违法违规收集使用个人信息专项治理的公告》，委托全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会（“App专项治理工作组”）开展专项治理工作。
- 2019年2月1日，信安标委发布《信息安全技术 个人信息安全规范（草案）》，向社会公开征求意见；2019年06月25日形成并公布征求意见稿，向社会公开征求意见；2020年3月6日正式公布并将于2020年10月1日起实施。
- 2019年3月1日，App专项治理工作组公布了《App违法违规收集使用个人信息自评估指南》；App运营者可参照指南对其收集使用个人信息的情况进行自查自纠，主动提升个人信息保护水平。

历史事件2

- 2019年3月15日，市场监管总局、中央网信办发布《关于开展App安全认证的公告》，公布《移动互联网引用程序（App）安全认证实施规则》，该规则指出App安全认证的认证依据是《个人信息安全规范》及相关标准、规范。App安全认证机构为中国网络安全审查技术与认证中心，监测机构由认证机构确定，App运营者自愿认证。
- 2019年5月5日，App专项治理工作组起草了《App违法违规收集使用个人信息行为认定方法（征求意见稿）》，《认定办法》已于2019年11月28日由中央网信办等四部委正式公布。
- 2019年5月28日，App专项治理工作组发布《App申请安卓系统权限机制分析与建议》。该文件是App专项治理工作组从主流安卓应用商店选取了100款下载量大、民众熟知和常用的App，对其申请安卓（Android）系统权限的情况进行分析并整理形成。

历史事件3

- 2019年6月1日，信安标委发布《网络安全实践指南—移动互联网应用基本业务功能必要信息规范（V1.0）》。
- 2019年8月8日，信安标委发布《信息安全技术 移动互联网应用（App）收集个人信息基本规范（草案）》并向社会公开征求意见；2019年10月25日更新草案，2020年01月20日公布《移动互联网应用（App）收集个人信息基本规范》征求意见稿，向社会公开征求意见。
- 2019年12月20日，App专项治理工作组发布《关于61款App存在收集使用个人信息问题的通告》。

历史事件4

- 2019年11月4日，工业和信息化部发布《关于开展App侵害用户权益专项整治工作的通知》，重点对四个方面八类问题开展规范整治工作，经历了企业自纠自查、监督抽查、结果处置三个阶段。最终分两批对存在问题的56款APP进行通报并限期整改，未整改的，已依法组织下架。值得注意的是，工信部在第二批通报中指出，“下一步，我部将以此次专项整治行动为契机，持续加强APP监督检查，形成常态化监管机制，切实维护用户权益。”

是否有隐私政策等收集使用规则

- 在App界面中能够找到隐私政策，包括通过弹窗、文本链接、附件、常见问题（FAQs）等形式，且隐私政策可正常显示。
- 隐私政策中需包含收集使用个人信息规则的相关内容。
- 隐私政策文本链接有效，且文本可正常显示。

是否提示用户阅读隐私政策等收集使用规则

- App需在首次运行或用户注册时通过弹窗等明显方式，提示用户阅读隐私政策。

- 避免使用灰色字体、缩小字号、键盘遮挡、置于边缘等方式未突出显示隐私政策链接。

隐私政策等收集使用规则是否易于访问

- 用户进入App主功能界面后，通过 4 次（含）以内的点击，能够访问到隐私政策。
- 在App常规交互界面展示隐私政策链接，避免仅在注册/登录界面展示隐私政策链接，或只能以咨询客服等方式查看隐私政策的情形。
- 隐私政策以单独成文的形式发布，而不是作为用户协议、用户说明等文件中的一部分存在。

隐私政策等收集使用规则是否易于阅读

- 隐私政策文本文字显示方式（字号、颜色、行间距、清晰度等）不会造成阅读困难。
- 需提供简体中文版隐私政策。
- 隐私政策的内容需符合通用的语言习惯，使用标准化的数字、图示，避免出现错别字或有歧义的语句。

是否公开App运营者的基本情况

- 隐私政策应对App运营者基本情况进行描述，至少包括组织或公司名称、注册地址或常用办公地址、个人信息保护工作机构或相关负责人联系方式。

是否公开收集使用个人信息的其他规则

- 隐私政策应说明发布、生效或更新日期。

- 隐私政策应对个人信息存放地域（境内、境外哪个国家或地区）、存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行明确说明。
- 如果App运营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。

- 如果存在个人信息出境情形，隐私政策中应将出境个人信息类型逐项列出并显著标识（如字体加粗、标星号、下划线、斜体、不同颜色等）；如果不存在个人信息出境情形，则明确说明。

是否公开收集使用个人信息的其他规则

- 隐私政策中应对App运营者在个人信息保护方面采取的措施和具备的能力进行说明，如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等。

- 如果存在个人信息对外共享、转让、公开披露等情况，隐私政策中应明确以下内容：①对外共享、转让、公开披露个人信息的目的；②涉及的个人信息类型；③接收方类型或身份。

- 隐私政策中应对以下用户权利和相关操作方法进行明确说明：①个人信息查询；②个人信息更正；③个人信息删除；④用户账户注销；⑤撤回已同意的授权。

是否公开收集使用个人信息的其他规则

- 隐私政策中至少提供以下一种申诉渠道：①电子邮件；②电话；③在线客服；④在线表单。

是否逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等

- 完整、清晰、区分说明各业务功能所收集的个人信息。隐私政策中所述内容应与App实际业务相符，并逐项说明各业务功能收集个人信息的目的、类型、方式，不应使用“等、例如”等方式不完整列举。

- 如App使用Cookie等同类技术（包括脚本、Clickstream、Web信标、Flash Cookie、内嵌 Web 链接等）收集个人信息，应向用户说明使用该类技术收集个人信息的目的、类型、方式。

是否逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等

- 如App嵌入了第三方代码、插件（如SDK）收集个人信息，应说明第三方类型，及收集个人信息的目的、类型、方式，说明方式包括隐私政策、弹窗提示、文字备注、文本链接等。

- 如委托的第三方或嵌入的第三方代码、插件直接将个人信息传输至境外的，应明确说明跨境传输个人信息的目的、类型和接收方等。

是否以适当的方式通知用户收集使用个人信息的目的、方式、范围发生的变化

- 收集使用个人信息的目的、方式和范围发生变化时，应以适当方式通知用户，适当方式包括更新隐私政策并以信息、邮件、弹窗等方式提醒用户阅读发生变化的条款等。

是否同步告知申请打开权限和要求提供个人敏感信息的目的

- 在申请打开可收集个人信息的权限时，App应通过显著方式（如弹窗提示等）同步告知用户其目的，对目的的描述应明确、易懂

- 注：常见可收集个人信息的系统权限有：
- iOS系统: 定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康；

- Android系统:日历、通话记录、相机、通讯录、位置、麦克风、电话、传感
- 器、短信、存储。

是否同步告知申请打开权限和要求提供个人敏感信息的目的

- 在要求用户提供个人敏感信息（用户身份证号、银行账号、行踪轨迹等）时，App应通过显著方式（如弹窗提示、文字备注、文本链接等）同步告知用户其目的，对目的的描述应明确、易懂。

- 注：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）未成年人的个人信息等。（该定义见GB/T
- 35273《个人信息安全规范》3.2 节）

收集使用规则是否易于理解

- 有关收集使用规则的内容应简练、结构清晰、重点突出，避免使用晦涩难懂的词语（如使用大量专业术语）和冗长繁琐的篇幅。

收集个人信息或打开可收集个人信息的权限前是否征得用户同意

- App收集个人信息前应提供由用户主动选择同意或不同意（包括退出、上一步、关闭、取消等）的选项。
- 未征得用户同意时，不应收集个人信息或打开可收集个人信息权限。如App首次打开时，在用户未得知收集个人信息的目的前，App就开始收集个人信息。
- 不应在征得用户同意前，利用Cookie等同类技术、或私自调用可收集用户个人信息的权限等方式收集个人信息

用户明确表示不同意收集后是否仍收集个人信息或打开可收集个人信息的权限

- 用户通过拒绝提供个人信息、不同意收集使用规则、拒绝提供或关闭权限等操作，明确拒绝App收集某类个人信息后，不应以任何形式收集该类个人信息或打开可收集个人信息的权限。

用户明确表示不同意收集后是否频繁征求用户同意、干扰用户正常使用

- 用户明确表示不同意收集后，不应在每次重新打开App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意收集个人信息。

- 用户明确表示不同意收集后，不应在每次重新打开App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意打开可收集个人信息的权限。

实际收集的个人信息或打开的可收集个人信息权限是否超出用户授权范围

- App收集使用个人信息的过程应与其所声明的隐私政策等收集使用规则保持一致。如实际收集的个人信息类型、申请打开的可收集使用个人信息的系统权限、调用系统权限函数的行为应与隐私政策所描述内容一致，不应超出隐私政策所述范围。

是否以默认选择同意隐私政策等非明示方式征求用户同意

- 在首次运行App或用户注册时，不应采用默认勾选隐私政策等非明示方式征求用户同意；

- 注册（包括登录即代表注册）的选项与同意隐私政策等的因果逻辑关系应清楚，且主动提示用户阅读以显著方式展示的隐私政策等收集使用规则后，执行下一步注册/登录等动作。

是否未经用户同意更改其设置的可收集个人信息权限状态

- 未经用户同意，不应私自更改用户设置的收集个人信息权限。
- App更新升级后，不应自动将用户设置的权限恢复到默认状态。

App利用用户个人信息和算法定向推送信息时，是否提供非定向推送信息的选项

- App存在利用用户个人信息和算法定向推送信息情形（包括利用个人信息和算法推送新闻和信息、展示商品、推送广告等），应提供拒绝接受定向推送信息，或者停止、退出、关闭相应功能的机制，或者不基于个人信息、用户画像等推送的模式、选项。

是否以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限

- App所明示收集使用个人信息的目的应真实、准确，不应故意欺瞒、掩饰收集使用个人信息的真实目的。如以红包、金币、抽奖等方式诱骗用户打开可收集个人信息的通讯录权限后，立即上传所有通讯录信息。

是否向用户提供撤回同意收集个人信息的途径、方式

- App应向用户提供撤回同意收集个人信息的途径、方式，并在隐私政策等收集使用规则中予以明确。
- 如用户拒绝或撤回特定业务功能收集个人信息的授权时，App不应暂停提供其他业务功能，或降低其他业务功能的服务质量。
- 如用户拒绝或撤回可收集个人信息的权限时，不得影响用户正常使用与该权限无关的功能，除非该权限是保证App正常运行所必需。

是否违反其所声明的收集使用规则，收集使用个人信息

- App应严格遵循其披露的隐私政策等收集使用规则，开展个人信息处理活动，如个人信息使用目的发生变化的，应再次征得用户同意。

是否收集与业务功能无关的个人信息

- 不应收集与业务功能无关的个人信息
- App不应申请打开与业务功能无关的可收集个人信息的权限。

用户是否可拒绝收集非必要信息或打开非必要权限

- App收集业务功能非必要的个人信息或申请打开非必要权限时，应征得用户同意，用户不同意不得拒绝提供相应业务功能。
- App不应将同意收集其他业务功能所需的个人信息或同意打开其他业务功能所需可收集个人信息权限，作为业务功能打开的前提条件。
- 如App提供无需注册即可使用（如浏览、游客模式）的业务模式，当用户拒绝支撑浏览、游客等模式以外的个人信息收集行为，App不应拒绝提供服务。

是否以非正当方式强迫收集用户个人信息

- 根据用户主动填写、点击、勾选等自主行为，作为App的各个业务功能打开或开始收集使用个人信息的条件。

- App新增业务功能申请收集的个人信息超出用户原有同意范围时，不应因用户拒绝新增业务功能收集个人信息的请求，拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外。

是否以非正当方式强迫收集用户个人信息

- 不应仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集其个人信息并以此作为提供服务的条件。

- App不得以捆绑方式强制要求用户一次性同意打开多个可收集个人信息权限。如将安卓版App的targetSdkVersion值设置低于 ，通过声明机制，在安装App时要求用户一次性同意打开多个可收集个人信息权限。

收集个人信息的频度是否超出业务功能实际需要

- App收集个人信息的频度不应超出业务功能实际需要，在使用App某业务功能过程中，应仅收集与当前业务功能相关的个人信息。
- 在未打开App或后台运行App时，App不应收集用户个人信息，除非App业务功能需要后台运行时继续提供服务，如导航功能。
- App接入第三方应用时，应提醒用户关注第三方应用收集使用个人信息的规则，不得私自截留第三方应用收集的个人信息。

向他人提供个人信息前是否征得用户同意

- 如App存在从客户端直接向第三方发送个人信息的情形，包括通过App客户端嵌入第三方代码、插件（如SDK）等方式，应事先征得用户同意，经匿名化处理的除外。
- 如个人信息传输至App服务器后，App运营者向第三方提供其收集的个人信息，应事先征得用户同意，经匿名化处理的除外。
- 如App接入第三方应用，当用户使用第三方应用时，应事先征得用户同意后，再向第三方应用提供个人信息，用户获知应用为第三方且在知悉收集使用个人信息规则后，自行同意提供给第三方的除外。

是否提供有效的注销用户账号功能

- App应提供有效的注销账号的途径（如在线操作、客服电话、电子邮件等），并在用户注销账号后，及时删除其个人信息或进行匿名化处理，法律法规另有规定的除外。

- 受理注销账号请求后，App运营者应在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。

- 注销账号的过程应简单易操作，不应设置不必要或不合理的注销条件，如提供额外的个人敏感信息用于身份验证，或未明确注销所需个人敏感信息在注销成功后是否会删除等。

是否提供有效的更正或删除个人信息

- App应提供有效的查询、更正、删除个人信息的途径。
- 用户无法通过在线操作方式及时响应个人信息查询、更正、删除请求的，App运营者应在承诺时限内（承诺时限不得超过15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。
- 查询、更正和删除个人信息的过程应简单易操作，不应设置不必要或不合理的条件。
- 用户更正、删除个人信息等操作完成时，App后台应同步执行完成相关操作。

是否建立并公布个人信息安全投诉、举报渠道

- App运营者应建立并公布可受理个人信息安全问题相关的投诉、举报渠道，受理可采取在线操作、客服电话、电子邮件等方式。

- App运营者应妥善受理用户关于个人信息相关的投诉、举报，并在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理。